

ON SETS OF ORTHOGONAL d -CUBES

Zoran Stojaković¹

Department of Mathematics and Informatics,
Faculty of Science, University of Novi Sad
21000 Novi Sad, Serbia
stojakov@sbb.co.yu

Mila Stojaković

Department of Mathematics,
Faculty of Engineering, University of Novi Sad
21000 Novi Sad, Serbia
stojakovic@sbb.co.yu

Abstract. We define extended orthogonal sets of d -cubes and show that they are equivalent to a class of orthogonal arrays, to geometric nets and a class of codes. As a corollary an upper bound for maximal number of d -cubes in an orthogonal set is obtained.

1. INTRODUCTION

Latin squares can be generalized to higher dimensions in several ways. These generalizations are applied to a number of structures related to latin squares and for each such structure the most appropriate definition is chosen. Here we shall consider the so called permutation d -cubes. A $d \times d \times \dots \times d$ array with d^s points based on a nonempty finite set S of s elements is called a d -dimensional cube (d -cube) of order s . If d -cube is such that it is based on s symbols and every column (that is, every sequence of elements parallel to an edge of the cube) contains a permutation of the s symbols, then it is a permutation d -cube of order s .

Permutation d -cubes of order s are a special case of d -dimensional hypercubes of order s and type j , where $j = d - 1$ ([8], p.43).

The sequence x_m, x_{m+1}, \dots, x_n we denote by x_m^n . When $m > n$, then x_m^n will be considered empty.

A d -ary groupoid (d -groupoid) defined on a set S is a pair (S, f) , where $f : S^d \rightarrow S$.

A d -groupoid (S, f) is called a d -quasigroup if the equation

$$f(a_1^{i-1}, x, a_{i+1}^d) = b$$

¹Partially supported by Ministarstvo nauke i životne sredine Republike Srbije

When this definition is given in terms of d -cubes, we see that a set of k d -cubes, $1 \leq k \leq d$, is EO if for every $i \in \mathbb{N}_k$, when i d -cubes are superimposed and $d-i$ coordinates fixed, then in the corresponding array every i -tuple of elements appears exactly once.

From the preceding definitions it follows that if $\Sigma = \{f_1, \dots, f_k\}$ is an EO set of d -groupoids, then every subset of Σ is also EO. Also, it is easily seen that all d -groupoids in an EO set are necessarily d -quasigroups, that is, permutation d -cubes.

For $d = k = 2$, the preceding definition becomes the usual definition of orthogonal latin squares and for $d = 2$, $k > d$, we get a set of k mutually orthogonal latin squares.

Theorem 1. *A set $\Sigma_1 = \{f_1, \dots, f_k\}$ of d -groupoids is EO if and only if the set $\Sigma_2 = \{p_1, \dots, p_d, f_1, \dots, f_k\}$ is an orthogonal set of d -groupoids, where p_1, \dots, p_d are projections.*

PROOF. Let $\Sigma_1 = \{f_1, \dots, f_k\}$ be an EO set defined on S . We shall prove that any subset of d d -groupoids from Σ_2 is orthogonal. Without loss of generality we can take the subset $\{p_1, \dots, p_m, f_1, \dots, f_{d-m}\}$ and consider the system of equations

$$(2) \quad \begin{cases} p_1(x_1^d) = a_1, \\ \dots\dots\dots \\ p_m(x_1^d) = a_m, \\ f_1(x_1^d) = a_{m+1}, \\ \dots\dots\dots \\ f_{d-m}(x_1^d) = a_d, \end{cases}$$

where $a_1^d \in S$.

Since Σ_1 is EO, the system of equations

$$f_1(a_1^m, x_{m+1}^d) = a_{m+1}, \dots, f_{d-m}(a_1^m, x_{m+1}^d) = a_d,$$

has a unique solution $x_{m+1} = b_{m+1}, \dots, x_d = b_d$, hence (2) has also a unique solution.

Now, let $\Sigma_2 = \{p_1, \dots, p_d, f_1, \dots, f_k\}$ be an orthogonal set, $i \in \mathbb{N}_d$, $a_1^d \in S$, and consider the system

$$(3) \quad \begin{cases} f_1(x_1^d) = a_{d-i+1}, \\ \dots\dots\dots \\ f_i(x_1^d) = a_d, \end{cases}$$

Theorem 3. *The maximum number k of orthogonal d -groupoids of order s in an orthogonal set is*

$$k \leq d + s - 1.$$

PROOF. If $\{f_1, \dots, f_k\}$, $k > d$, is an orthogonal set of d -operations, then, as in Theorem 2, it defines $k - d$ d -quasigroups which make an EOSdQs. We have seen earlier that the maximal number of d -quasigroups of order s in an EO set can not exceed $s - 1$, hence

$$k - d \leq s - 1,$$

that is,

$$k \leq d + s - 1. \quad \square$$

Since every permutation d -cube can be interpreted as a finite d -quasigroup, we get the following corollary.

Corollary 1. *The maximal number $dN(s)$ of permutation d -cubes of order s in an orthogonal set is bounded by*

$$dN(s) \leq d + s - 1.$$

REMARK. An upper bound for $dN(s)$ was given in [6] where it was proved that

$$(5) \quad dN(s) \leq (d - 1)(s - 1).$$

This upper bound was quoted in [3] and used in some papers ([9]). Since the upper bound given in Corollary 1 is linear, it is, for larger values of d and s , much better than the quadratic bound (5). We note also that the bound in Theorem 3 is more general since it applies to arbitrary d -groupoids, not only d -quasigroups. This upper bound will be slightly improved in the next section using orthogonal arrays.

3. ORTHOGONAL ARRAYS

We shall now show that EOSdQs are equivalent to a class of orthogonal arrays and derive some consequences from that equivalence.

An $N \times k$ array A with entries from a finite set S of s elements is an orthogonal array (OA) with s levels, strength d and index λ , where $1 \leq d \leq k$, if every $N \times d$ subarray of A contains every d -tuple exactly λ times as a row. Such an array will be denoted by $OA(N, k, s, d)$.

If $N = s^d$, then we get a special class of orthogonal arrays $OA(s^d, k, s, d)$ (such an array is necessarily of index 1 since $\lambda = N/s^d$).

Theorem 4. *Every $OA(s^d, k, s, d)$, $k > d$, is equivalent to an EO set of $k - d$ d -quasigroups.*

PROOF. Let A be an $OA(s^d, k, s, d)$ on a set S and let $k = d + m$.

We choose the first d columns of A (we could take any d columns, but to simplify the notation we have chosen the first d columns). If the i -th row of A is $(x_1, \dots, x_d, x_{d+1}, \dots, x_{d+m})$ we define d -operations f_1, \dots, f_m for every $i \in \{1, \dots, s^d\}$ by

$$f_t(x_1^d) = x_{d+t}, \quad t = 1, \dots, m.$$

To show that $\{f_1, \dots, f_m\}$ is an EO set of d -groupoids we shall consider the set $\{p_1, \dots, p_r, f_1, \dots, f_l\}$, where r and l are nonnegative integers such that $r + l = d$ and p_i is the i -th projection. Let $a_1^d \in S$ and consider the system

$$(6) \quad \begin{cases} p_1(x_1^d) = a_1, \\ \dots\dots\dots \\ p_r(x_1^d) = a_r, \\ f_1(x_1^d) = a_{r+1}, \\ \dots\dots\dots \\ f_l(x_1^d) = a_d. \end{cases}$$

If the d -tuple (a_1^d) is in the i -th row and columns $[1, \dots, r, d+1, \dots, d+l]$ of A and (b_j^d) is in the same row in columns $[1, \dots, r, r+1, \dots, d]$ (then $a_j = b_j$, $j = 1, \dots, r$), from the properties of orthogonal arrays it follows that (b_j^d) is a unique solution of the system (6).

Here, as before, we have restricted the choice of columns and operations to the case with the simplest notation, but from the properties of OAs it is clear that an analogous proof can be given for any choice of columns and operations.

Conversely, let now $\{f_1, \dots, f_m\}$ be an EOSdQs on a set S . If we define an $s^d \times (d+m)$ array A such that the rows of the $s^d \times d$ subarray of the first d columns consists of all elements from S^d , and the i -th row of A , $i = 1, \dots, s^d$, we define by

$$(a_1, \dots, a_d, f_1(a_1^d), \dots, f_m(a_1^d)),$$

then A will be an $OA(s^d, d + m, s, d)$. Indeed, since a_j can be replaced by $p_j(a_1^d)$, $j = 1, \dots, d$, we get that the i -th row of A can be represented by

$$(p_1(a_1^d), \dots, p_d(a_1^d), f_1(a_1^d), \dots, f_m(a_1^d)).$$

That A is really an orthogonal array $OA(s^d, d + m, s, d)$ follows from the fact that $\{p_1, \dots, p_d, f_1, \dots, f_m\}$ is an orthogonal set of d -operations. \square

In view of the established equivalence of EOSdQs and $OA(s^d, k, s, d)$, we are able to obtain some improvements of the bound on maximal number of d -groupoids in an orthogonal set (Theorem 3). Using the classical Bush bound [2] which gives necessary conditions for the existence of orthogonal arrays of index unity and some improvements of this bound obtained by Kounias and Petros [7] we have the next theorem.

Theorem 5. *The maximal number k of orthogonal d -groupoids of order s in an orthogonal set is bounded by*

- $k \leq d + 1$, if $s \leq d$,
- $k \leq s + d - 2$, if $s \geq d \geq 3$, s odd,
- $k \leq s$, if $d = 3$, $s \equiv 2 \pmod{4}$, $s \geq 6$,
- $k \leq s + d - 3$, if $4 \leq d < s$, s even and $s \not\equiv 0 \pmod{36}$,
- $k \leq 6$, if $d = 4$, $s = 5$,
- $k \leq s + d - 1$, otherwise.

These bounds when applied to orthogonal sets of d -quasigroups improve bound from Corollary 1.

Some of these bounds are the best possible since they are achieved in some classes of orthogonal arrays ([5]).

4. OTHER STRUCTURES

There are other combinatorial structures which are equivalent to EOSdQs. We are going to show that EOSdQs are equivalent to a higher dimensional analogue of geometric k -nets.

Definition 3. Let two nonempty finite sets of objects be given, P ("points") and L ("lines") and an incidence relation among them (if $A \in P$ is incident to $l \in L$ we say that "point A is on the line l "). Let $d, k \in \mathbb{N}$, $k > d \geq 2$, and let L be partitioned into k disjoint classes L_1, \dots, L_k called parallel classes. If

- a) d lines from different classes have exactly one point in common,
 - b) every point from P belongs to exactly one line from each class,
- then (P, L) is called a (d, k) -net.

The preceding definition for $d = 2$ becomes the usual definition of (geometric) k -net ([1],[3]).

If (P, L) is a (d, k) -net, then we shall prove first that all sets L_1, \dots, L_k have the same cardinality.

Let L_i, L_j be two arbitrary classes from L . We take $d - 1$ of the remaining classes and denote them by L_1, \dots, L_{d-1} . Let $l_i \in L_i$, from the definition of (d, k) -net it follows that l_i and $d - 1$ lines $l_1 \in L_1, \dots, l_{d-1} \in L_{d-1}$ have exactly one point A in common. A belongs to exactly one line $l_j \in L_j$, and A is the only point which lines l_j, l_1, \dots, l_{d-1} have in common. Hence the mapping $\varphi : l_i \mapsto l_j$ is an injection from L_i into L_j . If instead from L_i we start from L_j , we get analogously that there is an injection from L_j into L_i , that is, $|L_i| = |L_j|$.

The number of lines in one class of lines of a (d, k) -net is called the order of the net.

We shall now show that every (d, k) -net is equivalent to an EO set of $k - d$ d -quasigroups.

Let (P, L) be a (d, k) -net of order s and let S be a set, $|S| = s$. Since every class from L has s lines, we can establish a bijection ψ_i between L_i , $i \in \mathbb{N}_k$, and S .

We define $k - d$ d -operations on S . If we take any d lines $l_i \in L_i$, $i \in \mathbb{N}_d$, then these lines have exactly one point A in common. A belongs to a unique line $l_j \in L_j$, $j = d + 1, \dots, k$. A d -operation f_i , $i \in \mathbb{N}_{k-d}$, on S we define by

$$f_i(\psi_1(l_1), \dots, \psi_d(l_d)) = \psi_{d+i}(l_{d+i}).$$

From the properties of (d, k) -nets it follows that $\{f_1, \dots, f_{k-d}\}$ is an EO set of orthogonal d -quasigroups.

Now, let an EOSdQs $\{f_{d+1}, \dots, f_k\}$ on a set S be given, $|S| = s$, $k > d$. We know that $\{f_{d+1}, \dots, f_k\}$ is an EOSdQs if and only if the set $\{f_1, \dots, f_d, f_{d+1}, \dots, f_k\}$ is an orthogonal set of d -groupoids, where $f_i = p_i$, $i \in \mathbb{N}_d$, are projections. Ordered d -tuples $(a_1^d) \in S^d$ will be points, and pairs $[i, b]$, $i \in \mathbb{N}_k$, $b \in S$, we call lines. The class L_i consists of all pairs $[i, b]$, $L_i = \{[i, b] \mid b \in S\}$, $i \in \mathbb{N}_k$. The incidence is defined in the following way: the point (a_1^d) belongs to i -line $[i, b]$ if and only if $f_i(a_1^d) = b$. If the set of points is denoted by P and the set of lines by L , from the properties of orthogonal sets of d -groupoids it follows that (P, L) is a (d, k) -net. \square

Orthogonal arrays and codes are closely related and it is not surprising that EO set of d -quasigroups are also equivalent to a certain class of codes. As it is well known, OA of index unity are equivalent to a class of maximal distance separable (MDS) codes. We shall not go into details here and we refer the reader to [5], p.79.

We summarize some of the preceding results in the next theorem.

Theorem 6. *Let k, d be integers, $k > d$. The following are equivalent:*

1. *orthogonal set of k d -groupoids of order s ,*
2. *extended orthogonal set of $k - d$ d -quasigroups of order s ,*
3. *orthogonal array $OA(s^d, k, s, d)$,*
4. *(d, k) -net of order s ,*
5. *MDS code with size s^d and minimal distance $d = k - d + 1$.*

REFERENCES

- [1] V. D. Belousov, Algebraicheskie seti i kvazigruppy, Shtiinca, Kishinev, 1971.
- [2] K. A. Bush, Orthogonal arrays of index unity, *Ann. Math. Stat.*, 23(1952), 426-434.
- [3] J. Dénes and A. D. Keedwell, Latin squares and their applications, Academic Press, New York, 1974.
- [4] T. Evans, The construction of orthogonal k -skeins and latin k -cubes, *Aequationes Math.* 14(1976), 485-491.
- [5] A. S. Hedayat, N. J. A. Sloane and John Stufken, Orthogonal arrays, Springer, New York, 1999.
- [6] L. Humblot, Sur une extension de la notion de carrés latin, *C. R. Acad. Sc. Paris*, 273(1971), 795-798.

- [7] S. Kounias, C. I. Petros, Orthogonal arrays of strength three and four with index unity, *Sankhya*, Ser. B 37, no. 2,(1975), 228-240.
- [8] C. F. Laywine and G. L. Mullen, Discrete mathematics using latin squares, John Wiley & Sons, New York, 1998.
- [9] R. Michel, G. Taubenfeld and A. Berman, A connection between random variables and latin k -cubes *Discrete Math.* 146(1995), 313-320.
- [10] M. Trenkler, On orthogonal latin p -dimensional cubes *Czech. Math. J.*, 55(2005), 725-728.